SPYWOLF

Security Audit Report

Completed on

April 27, 2023

OVERVIEW

This audit has been prepared for **AmerG** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

AmerG

by GwaySBC

PROJECT DESCRIPTION

According to their whitepaper:

GwaySBC Protokol is an Ethereum smart contract platform that facilitates the stability of AmerG value by employing a series of Collateralized Secure Loan Smart Contracts or what we have innovated as Collateralized Secure Loan Smart Contracts (CSL).

GwaySBC Protokol is revolutionizing the world of Ethereum assets by letting anyone generate AmerG on the GwaySBC Platform. This generated AmerG can then be used like any other cryptocurrency - to make payments, send it to others or hold it as savings.

Release Date: Launched January, 2023

Category: Staking

CONTRACT 1 INFO

Token Name AmerG Stablecoin	Symbol AmerG
Contract Address 0x3963A62009C56634f9b5F115f8dB17C39D88B633	
Network Ethereum	Language Solidity
Deployment Date Jan 15, 2023	Verified? Yes
Total Supply 7,481	Status Not launched

TAXES

Buy Tax
none

Sell Tax
none

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	36
Uniq Senders	2
Uniq Receivers	22
Total Amount	286.61103152151776 AmerG
Median Transfer Amount	20 AmerG
Average Transfer Amount	286.61103152151776 AmerG
First transfer date	2023-01-16
Last transfer date	2023-04-02
Days token transferred	8

SMART CONTRACT STATS

Calls Count	7
External calls	7
Internal calls	0
Transactions count	1
Uniq Callers	2
Days contract called	8
Last transaction time	Apr-02-2023 01:42:35 AM +UTC
Created	Jan-15-2023 06:44:11 PM +UTC
Create TX	0x23fc70e3fd631a8089f09f04173c87b68ca12f408ff00939689e637a70c25219
Creator	0x702da91147d1ed27e4add88aa5d7dc95354cbca1

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Authorized user can mint new tokens.
This can lead to token's rapid inflation and liquidity drain.

```
function mint(address account, uint amount) external auth {
    _mint(account, amount);
}
```

⚠ Medium Risk

No medium risk-level threats found in this contract.

⚠ Low Risk

No low risk-level threats found in this contract.

Informational

Anyone can burn tokens if sufficient allowance is granted.

```
function burn(address account, uint amount) external {
    _spendAllowance(account, msg.sender, amount);
    _burn(account, amount);
}
```

Authorized user can add and remove authorized users.

```
function rely(address account) external auth {
    auths[account] = 1;

    emit Authorization(msg.sender, account, 1, block.timestamp);
}

function deny(address account) external auth {
    auths[account] = 0;

    emit Authorization(msg.sender, account, 0, block.timestamp);
}
```

Informational

Users can grant spend allowance via signature.
Be aware of dapps that require signature to login.

```
function permit(address holder, address spender, uint256 nonce, uint256 expiry,
                bool allowed, uint8 v, bytes32 r, bytes32 s) external
{
    bytes32 digest =
        keccak256(abi.encodePacked(
            "\x19\x01",
            DOMAIN_SEPARATOR,
            keccak256(abi.encode(PERMIT_TYPEHASH,
                                 holder,
                                 spender,
                                 nonce,
                                 expiry,
                                 allowed))
    ));

    require(holder != address(0), "holder invalid");
    require(holder == ecrecover(digest, v, r, s), "permit invalid");
    require(expiry == 0 || block.timestamp <= expiry, "permit expired");
    require(nonce == nonces[holder]++, "nonce invalid");
    uint amount = allowed ? type(uint256).max : 0;
    _approve(holder, spender, amount);
}
```

*Note
Be aware of dApps that require signature to log in.
Everyone that have the user's signature can approve the token from their behalf.

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

AmerG

GOOD PRACTICES FOUND

- ✔ The owner cannot stop or pause the contract
- ✔ The owner cannot set a transaction limit
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

CONTRACT 2 INFO

Token Name	Symbol
ETHVaultImplementationV1	N/A

Contract Address
0xAb9a4238a457640E7A9aE62C176b7f587D1bfD0b

Network	Language
Ethereum	Solidity

Deployment Date	Verified?
Feb 19, 2023	Yes

Total Supply	Status
N/A	Launched

TAXES

Buy Tax
none

Sell Tax
none

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

FOUND THREATS

⚠ High Risk

Owner can withdraw any tokens from the contract, including ETH.

```
function withdrawETH(uint256 amount) external payable onlyOwner {
    payable(_cold).transfer(amount);
}

function withdrawTokens(address token, uint256 amount) external payable onlyOwner {
    IERC20(token).transfer(_cold, amount);
}
```

Owner can set collateral percentage, refinance fees and interest rates without any limitations.

```
function setCollateralPercentages(uint256 minimum, uint256 maximum) external payable onlyOwner {
    minimumCollateralPercentage = minimum;
    maximumCollateralPercentage = maximum;
}

function setRefinanceFee(uint256 newRefinanceFee) external payable onlyOwner {
    refinanceFeePercentage = newRefinanceFee;
}

function setInterestRates(uint256[6] calldata newInterestRates) external payable onlyOwner {
    interestRates = newInterestRates;
}
```

FOUND THREATS

⚠ High Risk

Only contract’s owner can release the funds stacked by users.

```
function refundCollateral(uint256 vaultId) external payable onlyOwner {
    uint256 currentBalance = vaults[vaultId].amountCollateral;
    if(currentBalance == 0)
        revert INVALID_AMOUNT();

    vaults[vaultId].amountCollateral = 0;

    (bool ok, ) = vaults[vaultId].creator.call{value: currentBalance}("");
    require(ok);
}
```

CONTRACT 3 INFO

Token Name	Symbol
BTCVaultImplementationV1	N/A

Contract Address
0xE551B113B91cee0b7c8E51c5738Ca4c66014CA81

Network	Language
Ethereum	Solidity

Deployment Date	Verified?
Feb 19, 2023	Yes

Total Supply	Status
N/A	Launched

TAXES

Buy Tax
none

Sell Tax
none

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

FOUND THREATS

⚠ High Risk

Only contract's owner can release the funds stacked by users.

```
function refundCollateral(uint256 vaultId) external payable onlyOwner {
    uint256 currentBalance = vaults[vaultId].amountCollateral;
    if(currentBalance == 0) {
        revert INVALID_AMOUNT();
    }

    vaults[vaultId].amountCollateral = 0;

    BTC.transfer(vaults[vaultId].creator, currentBalance);
}
```

Owner can set collateral percentage, refinance fees and interest rates without any limitations.

```
function setCollateralPercentages(uint256 minimum, uint256 maximum) external payable onlyOwner {
    minimumCollateralPercentage = minimum;
    maximumCollateralPercentage = maximum;
}

function setRefinanceFee(uint256 newRefinanceFee) external payable onlyOwner {
    refinanceFeePercentage = newRefinanceFee;
}

function setInterestRates(uint256[6] calldata newInterestRates) external payable onlyOwner {
    interestRates = newInterestRates;
}
```

Owner can withdraw any tokens from the contract.

```
function withdrawTokens(address token, uint256 amount) external payable onlyOwner {
    IERC20(token).transfer(_cold, amount);
}
```

People can stake their ETH and wBTC and receive rewards in AmerG coin. Once users stake their collateral ETH and/or wBTC, only contract’s owner can release it.

TOKENOMICS

WEBSITE

Website URL
https://gwaysbc.app/

Domain Registry
https://www.tldregistrarsolutions.com/

Domain Expiration
2023-12-17

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

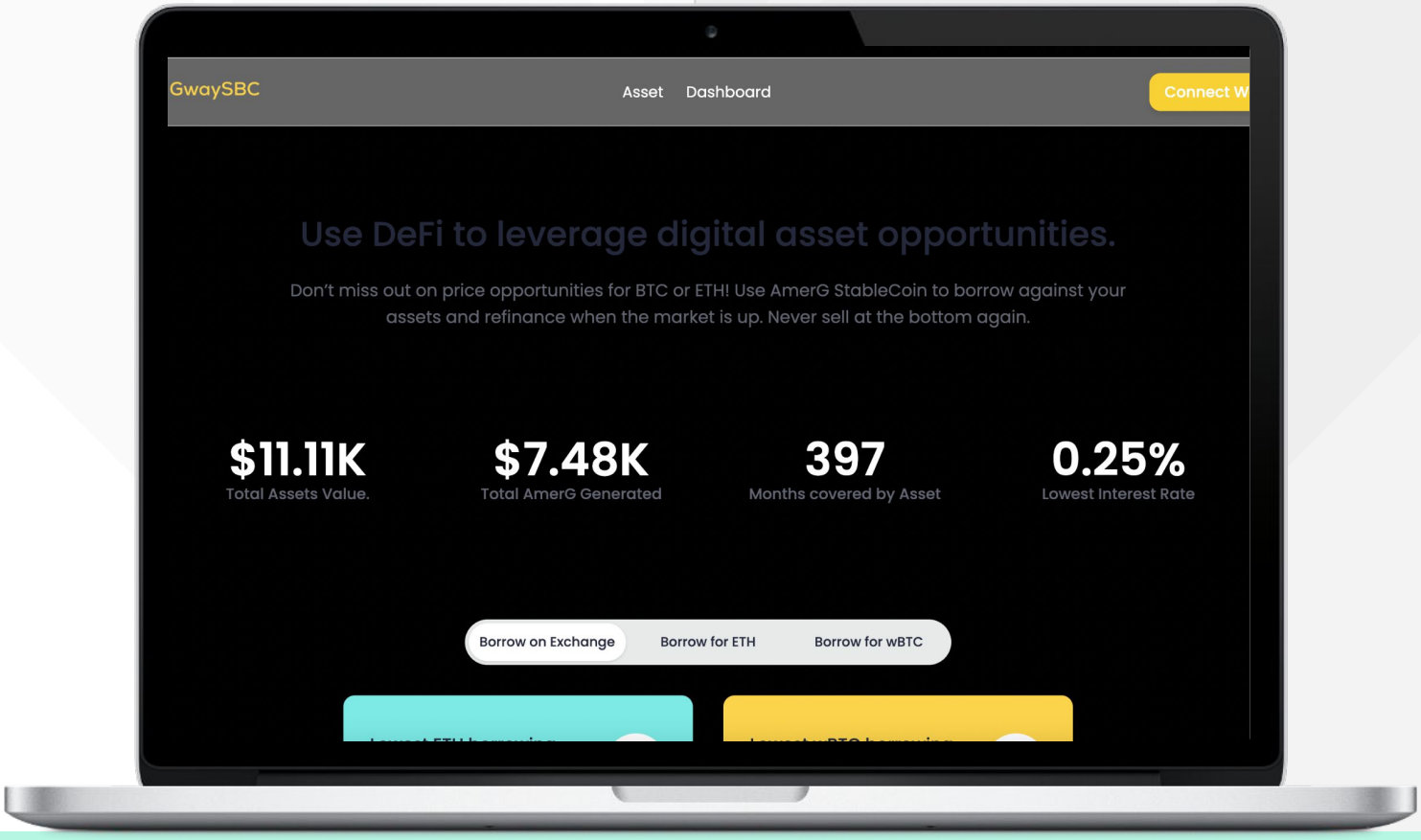
Design
Single page design with appropriate color scheme.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set with time frames.

Mobile-friendly?
Yes



gwaysbc.app

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active

Twitter

@GwaySbc

- 9 339 followers
- Posts frequently
- Active

Discord

- Not available

Telegram

@GwaySBC_Channel_Official

- 410 subscribers
- Announcement channel

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

Audits | KYCs | dApps
Contract Development

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.